CERT Advisory CA-1992-17 Hewlett-Packard NIS ypbind Vulnerability

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

==========
CA-92:17 CERT Advisory
October 5, 1992
Hewlett-Packard NIS ypbind Vulnerability

- ----------
*** SUPERSEDED BY CA-93:01 ***

The CERT Coordination Center has received information concerning a vulnerability in the NIS ypbind module for the Hewlett-Packard (HP) HP/UX Operating System for series 300, 700, and 800 computers.

HP is aware of the problem and has produced patches for HP/UX 8.xx versions. This problem is fixed in HP/UX 9.0.

Architecture	Patch ID	Filename	Checksum
Series 300	PHNE_1359	/hp-ux_patches/s300_400/8.X/PHNE_1359	39206 214
Series 700	PHNE_1360	/hp-ux_patches/s700/8.X/PHNE_1360	37915 299
Series 800	PHNE_1361	/hp-ux_patches/s800/8.X/PHNE_1361	44288 299

The checksums listed above are for the patch archive files from HP. Once unpacked, each shell archive contains additional checksum information in the file "patchfilename.text". This checksum is applicable to the binary patch file "patchfilename.updt".

These patches may be obtained from HP via ftp (this is NOT anonymous ftp) or the HP SupportLine. To obtain HP security patches, you must first register with the HP SupportLine. The registration instructions described below will not be included in future advisories.

If you have any questions about obtaining or installing the patches, contact the USA HP SupportLine at 415-691-3888, or your local HP SupportLine number. Please note that the telephone numbers in this advisory are appropriate for the USA and Canada.

- ----------

I. Description

A vulnerability in HP NIS allows remote NIS servers unauthorized access to local NIS hosts. An HP NIS client will accept ypset requests from hosts outside its NIS domain.

II. Impact

Root on a remote host running any vendor's implementation of NIS can gain root access on any local host running HP's NIS ypbind.

III. Solution

All HP NIS clients and servers running ypbind should obtain and install the patch, as detailed below.

The two sections below include the instructions for registering with the HP SupportLine and obtaining the HP security patches, and for installing the patch provided by HP. The instructions for installing the patch are also provided in the PHNE_xxxx.text file (this file is created after the patch has been unpacked).

==========
Beginning of Text provided by Hewlett-Packard
==========

HP SupportLine Registration Instructions

HP SupportLine phone number: 415-691-3888.

There are three categories for obtaining the security patches:

1) Eligible HP SupportLine customers (who have a software support contract or have recently purchased an HP 9000) who access via a terminal or modem.
2) Eligible HP SupportLine customers who would access via Internet.
3) Customers not currently accessing HP SupportLine.

For category 1:
- ---------------
Step 1: Dial 415-691-3680.

Step 2: When your communications program indicates that you are connected, press "return". The system prompt, ":" or "login:", should appear.

Step 3: If your system prompt is ":", log on to the HP SupportLine account by typing "HELLO USER.HPSL", followed by "return".
If your system prompt is "login:", log on by typing "login: hpsl", followed by "return".

Step 4: When prompted, type your system handle and password, each followed by "return". Both your system handle and password are provided in the cover letter you received with your "Getting Started Kit".

Step 5: Press "return" until the HP SupportLine Top Menu screen is displayed. If your terminal does not support block mode, you should enable HPSL's line editor by typing "SET EDITOR LINE" at the command prompt and entering "return".

For category 2:
- ---------------
Step 1: HP 9000, HP Apollo, and HP 64000 system users who have been authorized by the National Science Foundation (NSF) to use Internet may access HP SupportLine over the Internet. Connect to HP SupportLine using the address provided in your "Getting Started Kit". An example U.S. login is

```
telnet 192.6.148.19
       or
telnet support.mayfield.hp.com
```

Step 2: Once you access HP SupportLine, type "hpsl" at the "login:" prompt.

Step 3: When prompted, enter your system handle and password, each followed by "return". Both your system handle and password are provided in the cover letter you received with your "Getting Started Kit".

Step 4: Press "return" until the HP SupportLine Top Menu is displayed.

Step 5: At the Top Menu, choose "3 Patch support information" by typing "3" at the "Select an item or enter a command (? for help) :" prompt. This will put you in the Patch Support Information Menu.

Step 6: At the Patch Support Information Menu, choose "3 Retrieve patch file transfer login" to get your patch file transfer login by typing "3" at the "Select an item or enter a command (? for help) :" prompt. This will put you at a screen to choose the method for patch file transfers. The choices are ftp, kermit, and uucp. To choose ftp, type "1" at the "Enter selection :" prompt. The next screen will display your patch file transfer method and your patch file transfer login. You will use the *SAME* patch file login when you ftp patch file(s).

Step 7: When you exit the HP SupportLine, by typing "E" at the "Select an item or enter a command (? for help) :" prompt, the connection is closed.

Step 8: FTP to

```
192.6.148.19
     or
support.mayfield.hp.com
```

Step 9: At the "Name (support.mayfield.hp.com:username):" prompt, type your patch file transfer login.

Step 10: At the "Password:" prompt, type your password assigned to you by Hewlett-Packard when you registered.

Step 11: At the "ftp>" prompt, set the transfer mode to binary by typing "bin". You should get a message "Type set to I".

Step 12: At the "ftp>" prompt, cd to "hp-ux_patches". Then cd to the directory named for your type of architecture (s300_400, s700, or s800). Then cd to "8.X".

Step 13: At the "ftp>" prompt, type "get PHNE_xxxx" (where xxxx is
1359, 1360, or 1361 - depending on the architecture of your host(s)).

For category 3:
- ---------------
Step 1: Dial 415-691-3680.

Step 2: Type "hpslreg" at the "login:" prompt to begin the
registration process.

Step 3: Follow the instructional prompts.

Step 4: Once you have received your HP SupportLine system handle and
password, follow the directions in category 1) or 2), depending on
your preferred access method.

==
Patch Installation Instructions

Item Subject: PHNE_1359.text
Patch Name: PHNE_1359

Patch Description: ypbind that only accepts ypset from local host

This patch provides a special version of ypbind that only accepts
ypset requests from the local host. This prevents a superuser on a
remote system from issuing a ypset -h command to the local system to
create a rogue ypserver.

Path Name: /hp-ux_patches/s300_400/8.X/PHNE_1359

Effective Date: 920810

Patch Files:
    ypbind

SR#: 1650-172619

"what" string/timestamp:
    ypbind
        ypbind: $Revision: 1.2 $ $Date: 91/12/12 18:10:30
        $

"sum" output:
    46857 200 ypbind

Dependencies: None.

Supersedes: None.

Patch Package Size: 134 Kbytes

Installation Instructions:

     Please review all instructions and the Hewlett-Packard
     SupportLine User Guide or your Hewlett-Packard support terms
     and conditions for precautions, scope of license,
     restrictions, and, limitation of liability and warranties,
     before installing this patch.

     Note: Please back up your system before you patch.

- --
After getting the patch onto your machine, unshar the patch
(sh PHNE_1359).

To install this patch do the following:
1) Run the update program (Note: you must be logged in as root to
   update a system).
2) Once in the update "Main Menu" move the highlighted line to "Change
   Source or Destination ->" and press "Return" or "Select Item".
3) Make sure the highlighted item in the "Change Source or
   Destination" window is "From Tape Device to Local System ...", then
   press "Return" or "Select Item".
4) You should now be in the "From Tape Device to Local System" window.
   Change the "Source: /dev/rmt/0m" to "Source: /tmp/PHNE_1359.updt"
   (this assumes that you are in the /tmp directory where
   PHNE_1359.updt has been placed). Note: You must enter the complete
   path name.
5) Press "Done".
6) From here on follow the standard directions for update.

The customized script that update runs will move the original software

to /system/PHNE_1359/orig. HP recommends keeping this software there
in order to recover from any potential problems. It is also
recommended that you move the PHNE_1359.text file to /system/PHNE_1359
to be retained for future reference.

If you wish to put this patch on a magnetic tape and update from the
tape drive, dd a copy of the patch to the tape drive. As an example
the following will create a copy of the patch that update can read:
dd if=PHNE_1359.updt of=/dev/rmt/0m bs=2048

....

Item Subject: PHNE_1360.text
Patch Name: PHNE_1360

Patch Description: ypbind that only accepts ypset from local host

This patch provides a special version of ypbind that only accepts
ypset requests from the local host. This prevents a superuser on a
remote system from issuing a ypset -h command to the local system to
create a rogue ypserver.

Path Name: /hp-ux_patches/s700/8.X/PHNE_1360

Effective Date: 920810

Patch Files:
    ypbind

SR#: 1650-172619

"what" string/timestamp:
    ypbind
        ypbind: $Revision: 1.2 $ $Date: 91/12/12 18:10:30
        $

"sum" output:
    48068 256 ypbind

Dependencies: None.

Supersedes: None.

Patch Package Size: 164 Kbytes

Installation Instructions:

     Please review all instructions and the Hewlett-Packard
     SupportLine User Guide or your Hewlett-Packard support terms
     and conditions for precautions, scope of license,
     restrictions, and, limitation of liability and warranties,
     before installing this patch.

     Note: Please back up your system before you patch.

- --
After getting the patch onto your machine, unshar the patch
(sh PHNE_1360).

To install this patch do the following:
1) Run the update program (Note: you must be logged in as root to
   update a system).
2) Once in the update "Main Menu" move the highlighted line to "Change
   Source or Destination ->" and press "Return" or "Select Item".
3) Make sure the highlighted item in the "Change Source or
Destination" window is "From Tape Device to Local System ...", then
   press "Return" or "Select Item".
4) You should now be in the "From Tape Device to Local System" window.
   Change the "Source: /dev/rmt/0m" to "Source: /tmp/PHNE_1360.updt"
   (this assumes that you are in the /tmp directory where
   PHNE_1360.updt has been placed). Note: You must enter the complete
   path name.
5) Press "Done".
6) From here on follow the standard directions for update.

The customized script that update runs will move the original software
to /system/PHNE_1360/orig. HP recommends keeping this software there
in order to recover from any potential problems. It is also
recommended that you move the PHNE_1360.text file to /system/PHNE_1360
to be retained for future reference.

If you wish to put this patch on a magnetic tape and update from the
tape drive, dd a copy of the patch to the tape drive. As an example
the following will create a copy of the patch that update can read:

```
dd if=PHNE_1360.updt of=/dev/rmt/0m bs=2048

.....................................................................

Item Subject: PHNE_1361.text
Patch Name:  PHNE_1361

Patch Description: ypbind that only accepts ypset from local host

This patch provides a special version of ypbind that only accepts
ypset requests from the local host.  This prevents a superuser on a
remote system from issuing a ypset -h command to the local system to
create a rogue ypserver.

Path Name:  /hp-ux_patches/s800/8.X/PHNE_1361

Effective Date:  920810

Patch Files:
    ypbind

SR#:  1650-172619

"what" string/timestamp:
    ypbind
        ypbind:  $Revision: 1.2 $ $Date:  91/12/12 18:10:30
        $

"sum" output:
    48068 256 ypbind

Dependencies:  None.

Supersedes:  None.

Patch Package Size:  164 Kbytes

Installation Instructions:

     Please review all instructions and the Hewlett-Packard
     SupportLine User Guide or your Hewlett-Packard support terms
     and conditions for precautions, scope of license,
     restrictions, and, limitation of liability and warranties,
     before installing this patch.

     Note: Please back up your system before you patch.

- ----------------------------------------------------------------------------
After getting the patch onto your machine, unshar the patch
(sh PHNE_1361).

To install this patch do the following:
1) Run the update program (Note: you must be logged in as root to
   update a system).
2) Once in the update "Main Menu" move the highlighted line to "Change
   Source or Destination ->" and press "Return" or "Select Item".
3) Make sure the highlighted item in the "Change Source or
   Destination" window is "From Tape Device to Local System ...", then
   press "Return" or "Select Item".
4) You should now be in the "From Tape Device to Local System" window.
   Change the "Source:  /dev/rmt/0m" to "Source: /tmp/PHNE_1361.updt"
   (this assumes that you are in the /tmp directory where
   PHNE_1361.updt has been placed).  Note: You must enter the complete
   path name.
5) Press "Done".
6) From here on follow the standard directions for update.

The customized script that update runs will move the original software
to /system/PHNE_1361/orig.  HP recommends keeping this software there
in order to recover from any potential problems.  It is also
recommended that you move the PHNE_1361.text file to /system/PHNE_1361
to be retained for future reference.

If you wish to put this patch on a magnetic tape and update from the
tape drive, dd a copy of the patch to the tape drive.  As an example
the following will create a copy of the patch that update can read:
dd if=PHNE_1361.updt of=/dev/rmt/0m bs=2048

=============================================================================
                End of Text provided by Hewlett-Packard
=============================================================================

- ----------------------------------------------------------------------------
The CERT Coordination Center wishes to thank Brian Kelley of Ford
```

Motor Company for bringing this vulnerability to our attention. We
would also like to thank Hewlett-Packard for their response to this
problem.
- --

If you believe that your system has been compromised, contact the CERT
Coordination Center or your representative in FIRST (Forum of Incident
Response and Security Teams).

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
           CERT personnel answer 7:30 a.m.-6:00 p.m. EST(GMT-5)/EDT(GMT-4),
           on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Past advisories, information about FIRST representatives, and other
information related to computer security are available for anonymous ftp
from cert.org (192.88.209.5).

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQA/AwUBOBS9zlr9kb5qlZHQEQJcdACg1RK0w2q6eJarIGGINyUE9XgJqdEAnRAI
ayyywz5kO12rFjWBHBhqDJ7c
=MvvB
-----END PGP SIGNATURE-----